generating the trigger signal and the reset signal supplied to the hold step and the count step according to a second predetermined rule and/or at predetermined timing.

Frommer Lawrence & Haug LLP
745 Fifth Avenue
New York, NY 10151
212-588-0800
Customer Number 20999

AMENDMENTS TO THE DRAWINGS

The attached sheets of drawings include changes to Figures 1-5. These sheets replace the corresponding original sheets. The legend "Related Art" is added as a legend to each figure.

Attachment: Replacement Drawing Sheet 1 including Figure 1

Replacement Drawing Sheet 2 including Figure 2

Replacement Drawing Sheet 3 including Figure 3

Replacement Drawing Sheet 4 including Figure 4

Replacement Drawing Sheet 5 including Figure 5

Frommer Lawrence & Haug LLP
745 Fifth Avenue
New York, NY 10151
212-588-0800
Customer Number 20999

REMARKS/ARGUMENTS

Reconsideration and withdrawal of the rejections of the application are respectfully requested.

I. STATUS OF THE CLAIMS AND FORMAL MATTERS

Claims 1-9, 11-20, and 22 are pending in this application. Claims 10 and 21 have been canceled without prejudice or disclaimer of subject matter. No claims are amended in this paper.

No new matter has been introduced. It is submitted that these claims, as originally presented, were in full compliance with the requirements of 35 U.S.C. §112. Changes to claims are not made for the purpose of patentability within the meaning of 35 U.S.C. §101, §102, §103, or §112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled.

II. REJECTIONS UNDER 35 U.S.C. §103(a)

Claims 1-3, 9, 11-14, 20, and 22 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over U.S. Patent No. 5,345,508 to Lynn et al. (hereinafter, merely "Lynn") in view of "Concrete Security Analysis of CTR-OFB and CTR-OFB Modes of Operation" to Jaechul et al. (hereinafter, merely "Jaechul").

Claims 4-5 and 15-16 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over Lynn and Jaechul and further in view of U.S. Patent No. 7,242,772 to Tehranchi et al. (hereinafter, merely "Tehranchi").

Claims 6-8 and 17-19 were rejected under 35 U.S.C. §103(a), as allegedly unpatentable over Lynn, Jaechul, and Tehranchi and further in view of U.S. Patent No. 5,966,450 to Hosford et al. (hereinafter, merely "Hosford").

III. RESPONSE TO REJECTIONS UNDER 35 U.S.C. §103(a)

Claim 1 recites, *inter alia*:

"An encryption apparatus, comprising:

...**a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means**."
(emphasis added)

Applicants respectfully submit that Lynn, Jaechul, Tehranchi, and Hosford, taken either alone or in combination, fail to teach or suggest the above-identified features of claim 1. Specifically, nothing is found that discloses or teaches a path that inputs a part or all the encrypted data that are output from the calculation means to the hold means, as recited in claim 1.

The path of this invention transmits a part or all the encrypted data from the calculation means to the hold means of the encryption apparatus. Applicants submit that the path connects two means in the same encryption apparatus. The path of this invention, by transmitting encrypted data to the hold means in the same encryption apparatus, allows the encrypted data to be used in the encryption means.

The Office Action (see page 4) relies on column 5, lines 12-15 of Lynn to reject the above-identified features of claim 1. Specifically, the Office Action relies on a transmission of cipher text from an encryption device to a receiver to rejection the path of this invention.

Specifically, column 5, lines 9-24 of Lynn, reproduced below, describes:

"Various other logical functions can be equivalently used in place of XOR gate 16 to mask the identity of the key. This logical function need not be invertible. The XOR function is applied bitwise and is defined by a logical "0" whenever all inputs are the same, and a logical "1" otherwise. Initialization vector 14 is transmitted to receiver 20 as part of the communication sequence containing the ciphertext output 28. **Information transmitted from transmitter 10 to receiver 20 includes a block of ciphertext 28 concatenated with initialization vector 14. In essence, the initialization vector 14 becomes public in that it is transmitted in an unencrypted format and may be more easily appropriated by third parties**. However, since initialization vector 14 is always encoded with key 12 to produce temporal key 17, the value knowing of this initialization vector is limited. Since the initialization vector 14 is merely a component of temporal key 17, it would be difficult to determine the value of the temporal key knowing only the value of the initalization vector." (emphasis added)

Applicants respectfully submit that Lynn transmits cipher texts to a receiver, which is not included in the encryption device. Therefore, the transmission of Lynn among separated apparatus does not disclose or suggest the path that within the same encryption apparatus of this invention.

Therefore, independent claim 1 is patentable.

For reasons similar to, or somewhat similar to, those described above with regard to independent claim 1, claims 9, 11, 12, 20, and 22 are patentable.

IV. DEPENDENT CLAIMS

Each of the other claims in this application is dependent on an independent claim discussed above, and is therefore believed patentable for at least the same reasons presented for the independent claim upon which it depends. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

Similarly, because Applicants maintain that all claims are allowable for at least the reasons presented hereinabove, in the interests of brevity, this response does not comment on

each and every comment made by the Examiner in the Office Action. This should not be taken as acquiescence of the substance of those comments, and Applicants reserve the right to address such comments.

CONCLUSION

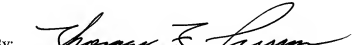
In the event the Examiner disagrees with any of statements appearing above with respect to the disclosures in the cited references it is respectfully requested that the Examiner specifically indicate those portions of the reference, or references, providing the basis for a contrary view.

Please charge any additional fees that may be needed, and credit any overpayment, to our Deposit Account No. 50-0320.

In view of the foregoing remarks, it is believed that all of the claims in this application are patentable and Applicants respectfully request early passage to issue of the present application.

Respectfully submitted,

Frommer Lawrence & Haug LLP
Attorneys for Applicants

By: 
Thomas F. Presson
Reg. No. 41,442
(212) 588-0800

Frommer Lawrence & Haug LLP
745 Fifth Avenue
New York, NY 10151
212-588-0800
Customer Number 20999